Retitalia S.p.A.
Via G.Gozzi, 1/A - 20129 Milano
+39 0249769100
www.retitalia.eu

Informativa Whistleblowing ai sensi
degli artt. 13 e 14 del Regolamento Europeo 2016/679

A) PREMESSA

Con questo documento vengono fornite informazioni circa il trattamento dei dati personali necessari alla gestione del "whistleblowing", ovvero l'istituto con il quale si assicura che il Segnalante (dipendente, collaboratore della Società o soggetto esterno, cd. whistleblower) di condotte illecite o di irregolarità di cui sia venuto a conoscenza in ragione del proprio rapporto di lavoro, sia soggetto ad una particolare tutela. E' importante chiarire che il trattamento dei dati personali nell'ambito del whistleblowing è conseguente alle previsioni normative e dunque la segnalazione del whistleblower deve integrare completamente, tanto da un punto di vista soggettivo che oggettivo, i requisiti che la qualificano come tale. In breve: il segnalante deve essere o un dipendente dell'Azienda o un lavoratore/collaboratore di una impresa fornitrice di beni o servizi dell'Azienda, o un libero professionista o consulente che presta la propria attività presso soggetti del settore pubblico o del settore privato, un volontario o tirocinante retribuito o non retribuito che presta la propria attività presso l'Azienda, un azionista o una persona con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza anche qualora tali funzioni siano esercitate in via di mero fatto presso soggetti del settore pubblico o del settore privato. La segnalazione deve avere ad oggetto comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che possono consistere in:

1) illeciti amministrativi, contabili, civili o penali che non rientrano nei successivi punti 3), 4), 5) e 6);
2) condotte illecite rilevanti ai sensi del D.lgs. 08 06 2001 n. 231 o violazioni dei modelli di organizzazione e gestione ivi previsti che non rientrano nei successivi punti n. 3), 4), 5) e 6);
3) illeciti che rientrano nell'ambito di applicazioni degli atti dell'unione Europea o nazionali;
4) atti ed omissioni che ledono gli interessi finanziari dell'Unione di cui all'art. 325 del trattato sul funzionamento dell'Unione Europea;
5) atti od omissioni riguardanti il mercato interno, di cui all'art. 26 par. 2 del Trattato sul funzionamento dell'Unione europea;
6) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei punti 3), 4) e 5).

La presente informativa viene pubblicata ai sensi e per gli effetti degli artt. 13 e 14 del Regolamento UE 2016/679 (in seguito GDPR), da Retitalia S.p.A., con sede in Milano via Gaspare Gozzi, 1- mail HR@retitalia.eu
-pec retitalia@legalmail.it e riguarda il trattamento dei dati personali raccolti mediante la procedura whistleblowing che la Società ha messo a disposizione di coloro (dipendenti, clienti, fornitori, partner commerciali, consulenti, collaboratori, ecc.) che intendono effettuare, secondo quanto previsto dalla procedura whistleblowing, una Segnalazione di condotte illecite in violazione della normativa nazionale o sovranazionale, di violazione del Codice Etico o del modello Organizzativo ex D. Lgs. 231/2001 e delle procedure interne adottate dalla Società, ai sensi e per gli affetti del D. Lgs. 24/2023.
La Società ha affidato le attività di ricezione e di gestione delle segnalazioni ad un organismo interno, ovvero all'Organismo di vigilanza ai sensi del D. Lgs. 231/2001 (OdV).

B) Titolare del trattamento

Titolare del Trattamento è Retitalia S.p.A., rappresentata dall'Amministratore Delegato pro tempore, contattabile all'indirizzo e-mail HR@retitalia.eu, con sede legale in Via Gaspare Gozzi 1/A — 20129 — Milano (MI).

C) Organismo di Vigilanza

L'Organismo di Vigilanza, nominato dalla Società ai sensi del D. Lgs. 231/2001, è contattabile ai seguenti recapiti: organismovigilanza@retitalia.eu oppure direttamente presso l'indirizzo della sede legale della Società in busta chiusa con dicitura esterna "riservata personale all'ODV di Retitalia Spa" in Via Gaspare Gozzi 1/A —20129 Milano.

D) Responsabile della Protezione dei Dati

La Società ha designato il Responsabile della protezione dei dati (RPD/DPO), che può essere contattato al seguente indirizzo email: gdpr@retitalia.eu

E) Tipologia di dati personali

Il Titolare tratterà i dati personali che il segnalante ha volontariamente fornito per rappresentare i fatti descritti nella segnalazione.

E.1.) Dati Comuni

Il Titolare raccoglierà e tratterà le informazioni che possono comprendere i dati personali del soggetto segnalante che volontariamente decida di fornirli quali il nome e cognome, codice fiscale, altri dati identificativi (telefono, indirizzo, mail etc.) o il ruolo aziendale, nonché ulteriori informazioni contenute nella segnalazione, ivi inclusi i dati personali del soggetto segnalato o delle persone comunque menzionate.
In ogni caso i dati personali contenuti nella segnalazione verranno trattati solo se pertinenti e necessari all'analisi dell'evento segnalato. I dati personali che manifestamente non sono utili alla gestione di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente perché inseriti erroneamente dal segnalante nella descrizione dei fatti oggetto di segnalazione, non sono trattati e, ove possibile, sono immediatamente cancellati, in applicazione del principio di minimizzazione dei dati personali.
Esulano dalle condotte segnalabili i fatti oggetto di vertenze di lavoro, anche in fase precontenziosa, nonché discriminazioni tra colleghi, conflitti interpersonali tra la persona segnalante ed un altro lavoratore o i superiori gerarchici, segnalazioni relative a trattamenti di dati effettuati nel contesto del rapporto individuale di lavoro in assenza di lesioni dell'interesse pubblico o dell'integrità della Società.
Non rientrano nell'ambito di applicazione oggettiva del D. Lgs. 24/2023 inoltre, le segnalazioni riferite a circostanze generiche o riconducibili ad una fase antecedente all'eventuale commissione di possibili illeciti, ovvero frutto di mere indiscrezioni o vociferazioni scarsamente attendibili, nonché a ipotesi di tentativo di reato.
In qualsiasi momento il segnalante può ritirare la segnalazione dandone comunicazione attraverso il medesimo canale utilizzato per effettuarla. In tal caso, i dati personali raccolti non saranno ulteriormente trattati, salvo sia già stato avviato un procedimento disciplinare e/o il Titolare abbia già comunicato tali dati ad un Autorità Giudiziaria secondo quanto previsto dal D. Lgs. 24/2023.

E.2) Dati particolari

La Società non è in grado di determinare a priori i dati oggetto della segnalazione, pertanto l'acquisizione e gestione delle Segnalazioni, anche attraverso atti e documenti in esse allegati, può dare luogo a trattamenti di dati personali anche particolari (ai sensi dell'art. 9 Regolamento UE 2016/679) quali dati sulla salute, dati sull'orientamento sessuale, appartenenza a credo religiosi etc., ovvero di dati relativi a condanne penali e reati (ai sensi dell'art. 10 Regolamento UE 2016/679).

F) Soggetti interessati dal trattamento

Gli Interessati dal trattamento dei dati possono essere:

- il Segnalante che volontariamente fornisce propri dati personali (dati personali raccolti presso l'Interessato);
- persone coinvolte nella segnalazione i cui dati personali vengono forniti dal segnalante nel contesto della descrizione del fatto segnalato, quali ad esempio persone indicate quali possibili responsabili (segnalato), testimoni, vittime, "facilitatore" (dati personali non ottenuti presso l'Interessato).

Il conferimento dei dati personali dal Segnalante è facoltativo: il Segnalante ha la facoltà di rimanere anonimo. Poiché tuttavia l'identità del segnalante potrebbe essere anche desunta da elementi di contesto o elementi della segnalazione, non potendosi così considerarla una segnalazione anonima in senso tecnico, in tal caso prevarrà comunque la volontà del segnalante di rimanere anonimo e sarà garantita la riservatezza della sua identità.

Il soggetto segnalante non è obbligato ad indicare nella segnalazione i dati personali del soggetto segnalato o di altre persone eventualmente coinvolte nella segnalazione.

G) Tutela dell'identità del Segnalante e consenso al suo disvelamento

L'identità del Segnalante e qualsiasi altra informazione da cui possa evincersi, direttamente o indirettamente tale identità, non saranno rivelate a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni (sempre nominate Incaricati), se non previo consenso espresso della persona segnalante e con le seguenti modalità:

1) Nell'ambito della procedura di segnalazione, qualora la conoscenza dell'identità della persona segnalante sia indispensabile anche ai fini della difesa dell'incolpato, l'identità potrà essere rivelata solo previo rilascio da parte del segnalante di apposito, libero ed informato consenso, nonché previa comunicazione scritta allo stesso delle motivazioni che richiedono il disvelamento della sua identità (art. 12 par. 2 e 6 D. Lgs. 24/2023). Il consenso del Segnalante al disvelamento della sua identità potrà essere revocato in qualsiasi momento, senza che ciò pregiudichi le liceità del trattamento, basato sul consenso, effettuato prima della revoca.

2) Nell'ambito di un procedimento disciplinare avviato nei confronti del presunto autore della condotta segnalata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa, l'identità della persona segnalante non può essere rivelata.

Qualora la contestazione dell'addebito disciplinare sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, l'identità potrà essere rilevata solo previo rilascio da parte del segnalante di apposito, libero ed informato consenso, nonché previa comunicazione scritta allo stesso delle motivazioni che richiedono il disvelamento della sua identità (art. 12 par. 5 e 6 D. Lgs. 24/2023).

Il consenso del segnalante al disvelamento della sua identità potrà essere revocato in qualsiasi momento, senza che ciò pregiudichi le liceità del trattamento, basato sul consenso, effettuato prima della revoca.

3) Nell'ambito del procedimento penale l'identità della persona segnalante è coperta dal segreto nei modi e nei limiti previsti dall'art. 329 del codice di procedura penale il quale prevede l'obbligo del segreto sugli atti compiuti nelle indagini preliminari sino a quando l'imputato non ne possa avere conoscenza e, comunque, non oltre la chiusura di tali indagini.

4) Nell'ambito di altri eventuali procedimenti giudiziari, l'identità della persona segnalante potrebbe essere disvelata per finalità di tutela del diritto di difesa dei soggetti incolpati.

H) Ulteriori necessità di consenso del soggetto segnalante

Quando, su richiesta della persona Segnalante, la segnalazione è effettuata in forma orale (tramite dispositivo telefonico oppure mediante incontro organizzato successivamente alla richiesta proposta all'indirizzo compliance@retitalia.eu e organismovigilanza@retitalia.eu dell'OdV), la segnalazione potrà essere documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale scritto, esclusivamente previo consenso specifico della

persona segnalante. In tal caso, la persona segnalante potrà verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione (art. 14 par. 4 D. Lgs. 24/2023).

I) Finalità del Trattamento

I dati personali sono trattati dal Titolare per le seguenti finalità:

a- gestione e verifica della segnalazione/denuncia effettuata ai sensi del D. Lgs. 24/2023 e adozione dei consequenziali necessari provvedimenti;

b- adempimento di obblighi previsti dalla legge o dalle Autorità di Vigilanza (quali D.Lgs. 231/2001, D. Lgs. 24/2023) o dalla normativa comunitaria;

c- difesa o accertamento di un diritto della Società in contenziosi civili, penali o amministrativi in relazione all'integrità dell'Ente privato ovvero del Titolare.

L) Base Giuridica del trattamento

Con riferimento ai punti a) e b) indicati nelle "Finalità del trattamento" le base giuridiche sono le seguenti:

-per il trattamento dei dati personali comuni, l'adempimento a un obbligo di legge cui è soggetto il Titolare ex art. 6 par. 1, lett. c) e par. 3 lett. a) e b) Regolamento UE 2016/679;

-per il trattamento dei dati personali particolari, l'adempimento a un obbligo di legge cui è soggetto il Titolare ex art. 9 par. 2, lett. g) Regolamento UE 2016/679;

- per il trattamento dei dati personali relativi a condanne penali e reati, l'adempimento a un obbligo di legge cui è soggetto il Titolare ex art. 10 par. 1, e art. 6 par 1 Regolamento UE 2016/679;

- per il trattamento dei dati che attiene alle operazioni connesse alla rivelazione della identità del soggetto segnalante di cui ai precedenti punti 1) e 2) indicati nella sezione "Tutela dei Dati del Segnalante", il consenso dell'Interessato ex art. 6 par. 1 lett. a) Regolamento UE 2016/679;

- per il trattamento dei dati che attiene alle operazioni di documentazione mediante registrazione o verbale scritto delle segnalazioni whistleblowing eseguite in forma orale, il consenso dell'Interessato ex art. 6 par. 1 lett. a) Regolamento UE 2016/679.

Con riferimento al punto c) indicato nella sezione "Finalità del trattamento" la base giuridica è il legittimo interesse del Titolare ex art. 6 par. 1) lett. f)

M) Modalità di trattamento

In relazione alle indicate Finalità, i dati personali saranno trattati:

-mediante strumenti manuali, informatici e telematici con logiche strettamente correlate alle finalità stesse e, comunque, con modalità tali da garantire la sicurezza, la riservatezza e la disponibilità dei dati stessi oltre al rispetto degli obblighi specifici sanciti dalla normativa;

-nel rispetto dei principi di liceità, correttezza, pertinenza e non eccedenza;

-da soggetti autorizzati all'assolvimento di tali compiti, costantemente identificati per iscritto, opportunamente istruiti e resi edotti dei vincoli imposti dalla normativa.

La documentazione in formato cartaceo è limitata al minimo indispensabile e archiviata e custodita in armadi e locali dotati di serrature di sicurezza.

La trasmissione dei dati forniti dalla persona segnalante mediante accesso alla piattaforma è gestita con protocollo HTTPS. Sono inoltre applicate tecniche di cifratura basate su Algoritmo AES e tutti i dati sono completamente criptati, garantendo in questo modo la riservatezza delle informazioni trasmesse. Non viene fatto uso di cookie per la trasmissione di informazioni di carattere personale, né vengono utilizzati cookie persistenti per il tracciamento degli utenti. Vengono utilizzati esclusivamente cookie tecnici nella misura strettamente necessaria al corretto ed efficiente utilizzo della piattaforma. L'uso dei cookie di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente della piattaforma. Il software GlobaLeaks segue le migliori pratiche standard della sicurezza settore ed è la miglior espressione quale risultato della ricerca applicata su di essa.

L'intera applicazione evita la registrazione di metadati sensibili che potrebbero portare all'identificazione degli informatori.

La riservatezza dell'autenticazione è protetta da Tor Onion Services v3 o TLS versione 1.2+

L'anonimato degli utenti è offerto mediante l'implementazione della tecnologia Tor. L'applicazione implementa un Onion Service v3 e consiglia agli utenti di utilizzare Tor Browser quando vi accedono.

Per prevenire o limitare le tracce forensi lasciate sul dispositivo utilizzato dai segnalanti e nei dispositivi coinvolti nella comunicazione la piattaforma utilizza l'intestazione HTTP Cache-control con la configurazione no-store per istruire i client e i possibili proxy di rete a disabilitare qualsiasi tipo di cache di dati.
Il modulo implementato dalla piattaforma utilizza l'attributo modulo HTMLS per indicare al browser di non mantenere la memorizzazione nella cache dei dati dell'utente al fine di prevedere e completare automaticamente i moduli negli invii successivi.
Accedendo all'interfaccia web di login, Amministratori e Destinatari dovranno inserire i rispettivi Nome Utente e Password. Se la password inviata è valida, il sistema concede l'accesso alle funzionalità disponibili a quell'utente secondo il ruolo che ne rappresenta.
I segnalanti accedono alle proprie segnalazioni utilizzando ricevute anonime, ovvero sequenze di 16 cifre generate casualmente dal backend al momento del primo invio della segnalazione. Il motivo di questo formato di 16 cifre è che assomiglia a un numero di telefono standard, rendendo più facile per gli informatori nascondere le proprie ricevute.
Le password non vengono mai memorizzate in chiaro ma il sistema mantiene a riposo solo un hash. Ciò si applica a tutti i segreti di autenticazione incluse le ricevute degli informatori.
La piattaforma memorizza le password degli utenti sottoposte ad hashing con un salt casuale a 128 bit, unico per ciascun utente.
Le password vengono sottoposte ad hashing utilizzando Argon2.
Il sistema impone l'utilizzo di password complesse implementando un algoritmo personalizzato necessario per garantire un'entropia ragionevole di ciascun segreto di autenticazione.
Il sistema implementa l'autenticazione a due fattori (2FA) basata su TOTP basata sull'algoritmo RFC 6238 e segreti a 160 bit.
Gli utenti possono registrarsi per 2FA tramite le proprie preferenze e gli amministratori possono facoltativamente imporre questo requisito.
Il sistema implementa una Proof of Work automatica ad ogni login che richiede ad ogni client di richiedere un token, risolvere un problema computazionale prima di poter effettuare un login o inviare una submission. L'implementazione della sessione segue le linee guida di sicurezza OWASP Session Management Cheat Sheet. Il sistema assegna una Sessione ad ogni utente autenticato. L'ID sessione è un segreto lungo 256 bit generato casualmente dal backend. Ogni sessione scade di conseguenza con un timeout di 60 minuti. Gli ID di sessione vengono scambiati dal client con il backend tramite un header (X-Session) e scadono non appena gli utenti chiudono il browser o la scheda su cui è in esecuzione GlobaLeaks. Gli utenti possono disconnettersi esplicitamente tramite un pulsante di disconnessione o implicitamente chiudendo il browser.
L'hash prevede una crittografia casuale per ciascun utente e una i segnalanti.
Tutte le notifiche vengono inviate tramite SMTP su canale crittografato TLS utilizzando SMTP/TLS o SMTPS, a seconda della configurazione.
I dati inviati, i file allegati, i messaggi e i metadati scambiati tra informatori e destinatari vengono crittografati utilizzando il protocollo di crittografia GlobaLeaks.
Oltre a questo GlobaLeaks implementa molti altri componenti di crittografia e quello che segue è l'insieme delle principali librerie e il loro utilizzo principale:

- Python-NaCL: viene utilizzato per implementare la crittografia dei dati

-PyOpenSSL: viene utilizzato per implementare HTTPS
Crittografia Python: viene utilizzata per implementare l'autenticazione

- Python-GnuPG: viene utilizzato per crittografare le notifiche e-mail e i download di file tramite "PGP'

La connessione degli utenti è sempre crittografata, tramite il Protocollo Tor durante l'utilizzo del Tor Browser oppure tramite TLS quando si accede all'applicazione tramite un comune browser.

L'uso di Tor è consigliato rispetto a HTTPS per le sue proprietà avanzate di resistenza all'intercettazione selettiva e alla censura che renderebbero difficile per una terza parte catturare o bloccare selettivamente l'accesso al sito a specifici informatori o dipartimenti aziendali.
Il software consente anche una facile configurazione di HTTPS offrendo sia la configurazione automatica tramite Let'sEncrypt che la configurazione manuale.
I certificati TLS vengono generati utilizzando la curva NIST P-384.
La configurazione abilita solo TLS1.2+ ed è ottimizzata e rafforzata per raggiungere il grado A+ di SSLLabs.

N) I Soggetti destinatari dei dati

Per il perseguimento delle Finalità suddette, i dati personali forniti sono resi accessibili solo a coloro i quali, all'interno della Società, sono competenti a ricevere o a dare seguito alle attività di analisi, istruttoria e gestione delle segnalazioni e di eventuali azioni conseguenti. Tali soggetti sono opportunamente istruiti al fine di evitare la perdita, l'accesso ai dati da parte di soggetti non autorizzati o trattamenti non consentiti dei dati stessi e, più in generale, in relazione agli obblighi in materia di protezione dei dati personali.
I dati personali oggetto della segnalazione potranno essere tuttavia comunicati, nell'ambito delle sole Finalità di sopra indicate, alle seguenti categorie di destinatari:

- Personale della Società incaricato dell'istruttoria e nominato Incaricato del trattamento;
- Consulenti esterni e Terze Parti con funzioni tecniche (ad esempio, il provider della piattaforma IT), che agiscono in qualità di Responsabili/Sub-Responsabili del trattamento e hanno sottoscritto un apposito contratto che disciplina puntualmente i trattamenti loro affidati e gli obblighi in materia di protezione dei dati e sicurezza del trattamento ai sensi dell'art. 28 GDPR;
- Società, enti, consorzi, professionisti che forniscano alla Società servizi elaborativi o che svolgono comunque attività connesse, strumentali o di supporto a quella oggetto della presente informativa;
- Autorità competenti in conformità a quanto previsto dall'art. 14 del D. Lgs. 24/2023 (Autorità Giudiziaria, Corte dei Conti e Autorità nazionale anticorruzione);
- Soggetti a cui la facoltà di accedere ai dati sia riconosciuta da disposizioni di legge (Istituzioni e/o Autorità Pubbliche, Autorità Giudiziaria, Organi di POlì2la).

L'elenco aggiornato dei soggetti destinatari dei dati può essere richiesto a: Area Compliance, Organismo di Vigilanza agli indirizzi mail: compliance@retitalia.eu e organismovigilanza@retitalia.eu

O) Diffusione dei dati

I dati personali oggetto del trattamento non saranno mai pubblicati, esposti o messi a disposizione/consultazione di soggetti indeterminati.

P) Conservazione dei dati

Fatti salvi diversi obblighi di legge, le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza. Ai sensi dell'art. 5 lett. d) D. Lgs. 24/2023 il termine per la conclusione della procedura è individuato in tre mesi dalla data dell'avviso di ricevimento della segnalazione iniziale, ovvero, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione iniziale.

Q) Trasferimento dei dati all'estero

I suoi dati personali non saranno trasferiti verso Paesi Terzi. Laddove venisse consentito l'accesso ai suoi dati personali da parte dei suddetti Paesi, verrebbero adottate le più stringenti misure di sicurezza logistico-informatiche atte a prevenire ed impedire il rischio di accesso ai medesimi da parte di soggetti non autorizzati o per finalità differenti di quelle sopra indicate.

R) Modalità di esercizio dei diritti e comunicazioni

L'interessato può esercitare i suoi diritti contattando il Responsabile "interno" al trattamento dei dati sig.ra Elisa Iacoponi presso la sede legale dell'Azienda, oppure mediante richiesta scritta inviata al Titolare del trattamento presso la sede in Milano oppure inviando una mail all'indirizzo di posta elettronica già indicata sopra.

S) Diritti degli Interessati

Il Regolamento UE 2016/679 (artt. da 15 a 22) conferisce agli Interessati l'esercizio di specifici diritti. In particolare, in relazione al trattamento dei propri dati personali oggetto della presente informativa, l'interessato ha diritto di chiedere a Retitalia S.p.A.:

l'accesso: l'interessato può chiedere conferma che sia o meno in essere un trattamento di dati che lo riguardi, oltre a maggiori chiarimenti circa le informazioni di cui alla presente informativa;
la rettifica: l'interessato può chiedere di rettificare o integrare i dati che ha fornito, qualora inesatti o incompleti;
la cancellazione: l'interessato può chiedere che i suoi dati vengano cancellati, qualora non siano più necessari alle suddette finalità, in caso di revoca del consenso o sua opposizione al trattamento, in caso di trattamento illecito, ovvero sussista un obbligo legale di cancellazione;
la limitazione: l'interessato può chiedere che i suoi dati siano trattati solo ai fini della conservazione, con esclusioni di altri trattamenti, per il periodo necessario alla rettifica dei suoi dati, in caso di trattamento illecito per il quale si oppone alla cancellazione, qualora debba esercitare i suoi diritti in sede giudiziaria e i dati conservati possano essere utili e, infine, in caso di opposizione al trattamento e sia in corso una verifica sulla prevalenza dei motivi legittimi di Retitalia S.p.A. rispetto ai suoi; l'opposizione: l'interessato può opporsi in qualunque momento al trattamento dei suoi dati, salvo che vi siano motivi legittimi per procedere al trattamento che prevalgano sui suoi, per esempio per l'esercizio o la difesa in sede giudiziaria;
la portabilità: l'interessato può chiedere di ricevere i suoi dati, o di farli trasmettere ad altro titolare dallo stesso indicato, in un formato strutturato, di uso comune e leggibile da dispositivo automatico.
Inoltre, l'Interessato ha diritto di proporre reclamo qualora ritenga che i suoi diritti siano stati violati, all'Autorità di Controllo che in Italia è il Garante per la Protezione dei Dati Personali.
Ai sensi dell'articolo 2-undecies del D.Lgs. n. 196/2003 e s.m.i. (di seguito "Nuovo Codice Privacy") ed in attuazione dell'articolo 23 del GDPR, si informa che i summenzionati diritti non possono essere esercitati da parte delle persone coinvolte nella segnalazione, qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona segnalante.
In particolare, l'esercizio di tali diritti:
sarà effettuabile conformemente alle disposizioni di legge o di regolamento che regolano il settore (D.Lgs. 24/2023);
potrà essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'Interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'Interessato, al fine di salvaguardare la riservatezza dell'identità della persona segnalante;
in tali casi, i diritti dell'Interessato possono essere esercitati anche tramite il Garante per la Protezione dei Dati Personali con le modalità di cui all'art. 160 del Nuovo Codice Privacy, nel qual caso il Garante informa l'Interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del suo diritto a proporre ricorso giurisdizionale.
In qualsiasi momento, l'Interessato potrà chiedere di esercitare i suoi diritti a Retitalia S.p.A. rivolgendosi all'indirizzo mail info@retitalia.eu o all'indirizzo email del DPO gdpr@retitalia.eu

RETITALIA S.P.A.
Amministratore Delegato
Dr. Dario Falchi